

# Application of Information Theory, Lecture 9

## Parallel Repetition of Interactive Arguments

**Handout Mode**

Iftach Haitner

Tel Aviv University.

December 23, 2014

# Part I

## **Interactive Proofs and Arguments**

# $\mathcal{NP}$ as a Non-interactive Proofs

## Definition 1 ( $\mathcal{NP}$ )

$\mathcal{L} \in \mathcal{NP}$  iff  $\exists$  and poly-time algorithm  $V$  such that:

- ▶  $\forall x \in \mathcal{L}$  there exists  $w \in \{0, 1\}^*$  s.t.  $V(x, w) = 1$
- ▶  $V(x, w) = 0$  for every  $x \notin \mathcal{L}$  and  $w \in \{0, 1\}^*$

Only  $|x|$  counts for the running time of  $V$ .

This proof system has

- ▶ Efficient verifier, efficient prover (given the witness)
- ▶ Soundness holds unconditionally

# Interactive proofs/arguments

Protocols between **efficient** verifier and **unbounded/efficient** prover.

## Definition 2 (Interactive proof)

A protocol  $(P, V)$  is an **interactive proof** for  $\mathcal{L}$ , if  $V$  is a **PPT** and:

**Completeness**  $\forall x \in \mathcal{L}$ :  $\Pr[(P, V)(x) = 1] \geq 2/3$ .

**Soundness**  $\forall x \notin \mathcal{L}$ , and **any** algorithm  $P^*$ :  $\Pr[(P^*, V)(x) = 1] \leq 1/3$ .

**IP** is the class of languages that have interactive proofs.

- ▶ **IP = PSPACE!**
- ▶ The above protocol has **completeness error**  $\frac{1}{3}$ , and **soundness error**  $\frac{1}{3}$
- ▶ We typically consider achieve (directly) perfect completeness.
- ▶ Smaller “soundness error” achieved via repetition.
- ▶ Relaxation: **interactive arguments** [also known as, **Computationally sound proofs**]: soundness only guaranteed against **efficient** (PPT) provers.
- ▶ Games — no-input protocols.

# Section 1

## **Interactive Proof for Graph Non-Isomorphism**

# Graph isomorphism

$\Pi_m$  – the set of all permutations from  $[m]$  to  $[m]$

## Definition 3 (graph isomorphism)

Graphs  $G_0 = ([m], E_0)$  and  $G_1 = ([m], E_1)$  are **isomorphic**, denoted  $G_0 \equiv G_1$ , if  $\exists \pi \in \Pi_m$  such that  $(u, v) \in E_0$  iff  $(\pi(u), \pi(v)) \in E_1$ .

- ▶  $\mathcal{GI} = \{(G_0, G_1) : G_0 \equiv G_1\} \in \mathcal{NP}$
- ▶ Does  $\mathcal{GNI} = \{(G_0, G_1) : G_0 \not\equiv G_1\} \in \mathcal{NP}$ ?
- ▶ We will show a simple interactive proof for  $\mathcal{GNI}$   
Idea: Beer tasting...

## Interactive proof for $\mathcal{GNI}$

**Protocol 4**  $((P, V)(G_0 = ([m], E_0), G_1 = ([m], E_1)))$

1.  $V$  chooses  $b \leftarrow \{0, 1\}$  and  $\pi \leftarrow \Pi_m$ , and sends  $\pi(E_b)$  to  $P$ .<sup>a</sup>
2.  $P$  send  $b'$  to  $V$  (tries to set  $b' = b$ ).
3.  $V$  accepts iff  $b' = b$ .

---

$$^a \pi(E) = \{(\pi(u), \pi(v)) : (u, v) \in E\}.$$

### Claim 5

The above protocol is  $\text{IP}$  for  $\mathcal{GNI}$ , with perfect completeness and soundness error  $\frac{1}{2}$ .

## Proving Claim 5

- ▶ Graph isomorphism is an equivalence relation (separates the set of all graph pairs into separate subsets)
- ▶  $([m], \pi(E_i))$  is a random element in  $[G_i]$  — the equivalence class of  $G_i$

Hence,

$$G_0 \equiv G_1: \Pr[b' = b] \leq \frac{1}{2}.$$

$$G_0 \not\equiv G_1: \Pr[b' = b] = 1 \text{ (i.e., } P \text{ can, possibly inefficiently, extracted from } \pi(E_i))$$

□



## Part II

# Hardness Amplification

# Hardness amplification

- ▶ In most settings we need **very small** soundness error (i.e., close to 0)
- ▶ Typically done by “amplifying the security” of an interactive proof/argument of **large** soundness error.
- ▶ Two main approaches:
  - ▶ **Sequential** repetition: achieves optimal amplification rate in almost any computation model, but increases the round complexity
  - ▶ **Parallel** repetition: sometimes does not achieve optimal amplification rate and sometimes achieves **nothing**
- ▶ How come parallel repetition might not work? **Example**
- ▶ Parallel repetition **does** achieve optimal amplification rate for interactive proofs and public-coin interactive arguments
- ▶ Public-coin interactive proof/argument — in each round the verifier flips coins and sends them to the prover. To compute its output, the verifier applies some (fixed) function to the protocol’s transcript.

## Hardness amplification, cont

- ▶ Give a protocol  $\pi = (P, V)$  and  $k \in \mathbb{N}$ , let  $\pi^{(k)} = (P^{(k)}, V^{(k)})$  be the  $k$ -fold parallel repetition of  $\pi$ : i.e.,  $k$  parallel independent copies of  $\pi$
- ▶ Assume  $\Pr[(\tilde{P}, V) = 1] \leq \varepsilon$  for any  $t$ -time algorithm  $\tilde{P}$ , we would like to prove that  $\Pr[(\widetilde{P^{(k)}}^{(k)}, V^{(k)}) = 1^k] \leq f(\varepsilon)$  for any  $t'$ -time algorithm  $\widetilde{P^{(k)}}^{(k)}$ .
- ▶ Typically,  $t' = t \cdot \text{poly}(f(\varepsilon)/k)$
- ▶ If  $f(\varepsilon) = \varepsilon^{\Omega(k)}$ , the above is an exponential-rate amplification (and hence optimal)
- ▶ If  $f(\varepsilon) = \varepsilon^{\delta_1 \cdot k^{\delta_2}}$ , the above is a weakly-exponential-rate amplification
- ▶ Why time?
- ▶ Concrete security
- ▶ In the following we focus on games (no input protocols)

## Section 2

# **Parallel repetition of public-coin interactive argument**

# Parallel repetition of public-coin interactive argument

## Theorem 6

Let  $\pi = (P, V)$  be  $m$ -round,  $t_\pi$ -time, public-coin protocol with  $\Pr[(\tilde{P}, V) = 1] \leq \varepsilon$  for any  $t$ -time  $\tilde{P}$ , then  $\Pr[(\widetilde{P^{(k)}}, V^{(k)}) = 1^k] \leq \varepsilon^{k/4}$  for any  $t \cdot \frac{\varepsilon^{k/4}}{mk^3 t_\pi}$ -time  $\widetilde{P^{(k)}}$ .

Proof plan: Let  $\widetilde{P^{(k)}}$  be  $t'$ -time algorithm with  $\Pr[(\widetilde{P^{(k)}}, V^{(k)}) = 1^k] = \varepsilon^{(k)}$ , we construct  $t' \cdot \frac{2mk^2 t_\pi \log \frac{1}{\varepsilon^{(k)}}}{\varepsilon^{(k)}}$ -time  $\tilde{P}$  with  $\Pr[(\tilde{P}, V) = 1] \geq (\varepsilon^{(k)})^{4/k}$ .

- ▶ The  $k/4$  in the exponent can be pushed to be almost  $k$ .
- ▶ Assume for simplicity that  $\widetilde{P^{(k)}}$  is deterministic
- ▶ Assume wlg. that  $V$  sends the first message in  $\pi$  and that in each round it samples and sends  $\ell$  coins.
- ▶ We view the coins of  $V^{(k)}$  as a matrix  $R \in \{0, 1\}^{m \times \ell}$ , letting  $R_j$  denote the coins of the  $j$ 'th round, and  $R_{1, \dots, j}$  the coins of the first  $j$  rounds.
- ▶ Let  $R \sim \{0, 1\}^{m \times \ell}$

## Algorithm $\tilde{P}$

Let  $q = 2k \cdot \log \frac{1}{\varepsilon^{(k)}}$ .

### Algorithm 7 ( $\tilde{P}$ )

1. Let  $i^* \leftarrow [k]$ .
2. Upon getting the  $j$ 'th message  $r$  from  $V$ , do:
  - 2.1 Let  $R \leftarrow \{0, 1\}^{m \times \ell}$ , conditioned that  $R_{1, \dots, j-1} = \tilde{R}_{1, \dots, j-1}$  and  $R_{j, i^*} = r$ .
  - 2.2 If  $(\widetilde{P^{(k)}}, V^{(k)}(R)) = 1^k$ :
    - 2.2.1 Set  $\tilde{R}_j = R_j$
    - 2.2.2 Send  $a_{j, i^*}$  back to  $V$ , for  $a_j$  being the  $j$ 'th message  $\widetilde{P^{(k)}}$  send to  $V^{(k)}$  in  $(\widetilde{P^{(k)}}, V^{(k)}(R))$ .
  - Else, GOTO Line 2.1
- 2.3 Abort if the overall number of sampling exceeds  $\lceil qm/\varepsilon^{(k)} \rceil$ .

- ▶ Let  $\tilde{P}'$  be the non aborting variant of  $\tilde{P}'$ , let  $\tilde{R}$  and  $\tilde{N}$  be the value of  $\tilde{R}$  and  $\#$  of samples done in a random execution of  $(\tilde{P}', V^{(k)})$ .
- ▶  $\Pr \left[ (\tilde{P}, V) = 1 \right] \geq \Pr \left[ \text{win}(\tilde{R}, \tilde{N}) := (\widetilde{P^{(k)}}, V^{(k)}(\tilde{R})) = 1^k \wedge \tilde{N} \leq qm/\varepsilon^{(k)} \right]$ .

# Ideal “attacker”

## Experiment 8 ( $\hat{P}$ )

For  $j = 1$  to  $m$ :

1. Let  $R \leftarrow \{0, 1\}^{m \times \ell}$ , conditioned that  $R_{1,\dots,j-1} = \hat{R}_{1,\dots,j-1}$ .
2. If  $(\widetilde{P^{(k)}}, V^{(k)}(R)) = 1^k$ , set  $\hat{R}_j = R_j$ . Else, GOTO Line 1.

- ▶ Let  $\hat{R}$  be the value of  $\hat{R}$  in the end of a random execution of  $\hat{P}$ .
- ▶  $\hat{R} \sim R|_{(\widetilde{P^{(k)}}, V^{(k)}(R))=1^k}$
- ▶ In particular,  $\Pr \left[ (\widetilde{P^{(k)}}, V^{(k)}(\hat{R})) = 1^k \right] = 1$
- ▶ Let  $\hat{N}$  be # of samples done in  $\hat{R}$ .

## Lemma 9

$$\Pr \left[ \hat{N} \leq qm/\varepsilon^{(k)} \right] \geq 1 - \frac{1}{q}$$

## Proving Lemma 9

- ▶ Let  $(X_1, \dots, X_m) = \mathbf{R}$  and  $(Y_1, \dots, Y_m) = \widehat{\mathbf{R}}$
- ▶  $v(\mathbf{y} = (y_1, \dots, y_j)) := \Pr \left[ (\widetilde{\mathbf{P}}^{(k)}, V^{(k)}(X^m)) = 1^k \mid X^j = \mathbf{y} \right]$   
(letting  $X^j = (X_1, \dots, X_j)$ )
- ▶ Conditioned on  $Y^j = \mathbf{y} = (y_1, \dots, y_j)$ , the expected # of samples done in  $(j+1)$ 'th round of  $\widehat{\mathbf{P}}$  is  $\frac{1}{v(\mathbf{y})}$ .
- ▶ We prove Lemma 9 showing that  $\mathbb{E} \left[ \frac{1}{v(Y^j)} \right] = \frac{1}{\varepsilon^{(k)}}$  for every  $j \in \{0, \dots, m-1\}$

### Claim 10

For  $j \in \{0, \dots, m-1\}$  and  $\mathbf{y} \in \text{Supp}(Y^j)$  it holds that  $\Pr_{Y^j}[\mathbf{y}] = \Pr_{X^j}[\mathbf{y}] \cdot \frac{v(\mathbf{y})}{\varepsilon^{(k)}}$

$$\begin{aligned} \text{Hence, } \mathbb{E}_{Y^j} \left[ \frac{1}{v(Y^j)} \right] &= \sum_{\mathbf{y} \in \text{Supp}(Y^j)} \Pr[Y^j = \mathbf{y}] \cdot \frac{1}{v(\mathbf{y})} \\ &= \sum_{\mathbf{y}} \Pr[X^j = \mathbf{y}] \cdot \frac{v(\mathbf{y})}{\varepsilon^{(k)}} \cdot \frac{1}{v(\mathbf{y})} = \frac{1}{\varepsilon^{(k)}} \cdot \sum_{\mathbf{y} \in \text{Supp}(Y^j)} \Pr[X^j = \mathbf{y}] = \frac{1}{\varepsilon^{(k)}}. \quad \square \end{aligned}$$



## Proving Claim 10

Note that

$$\begin{aligned}\Pr_{Y_j | Y^{j-1} = \mathbf{y}_{1, \dots, j-1}}[y_j] &= \sum_{\ell=1}^{\infty} (1 - v(\mathbf{y}_{1, \dots, j-1}))^{\ell-1} \cdot \Pr_{X_j | X^{j-1} = \mathbf{y}_{1, \dots, j-1}}[y_j] \cdot v(\mathbf{y}) \quad (1) \\ &= \frac{1}{v(\mathbf{y}_{1, \dots, j-1})} \cdot \Pr_{X_j | X^{j-1} = \mathbf{y}_{1, \dots, j-1}}[y_j] \cdot v(\mathbf{y})\end{aligned}$$

The proof proceeds by induction on  $j$ .

$$\begin{aligned}\Pr_{Y^j}[\mathbf{y}] &= \Pr_{Y^{j-1}}[\mathbf{y}_{1, \dots, j-1}] \cdot \Pr_{Y_j | Y^{j-1} = \mathbf{y}_{1, \dots, j-1}}[y_j] \\ &= \Pr_{X^{j-1}}[\mathbf{y}_{1, \dots, j-1}] \cdot \frac{v(\mathbf{y}_{1, \dots, j-1})}{\varepsilon^{(k)}} \cdot \Pr_{Y_j | Y^{j-1} = \mathbf{y}_{1, \dots, j-1}}[y_j] \quad (\text{i.h.}) \\ &= \Pr_{X^{j-1}}[\mathbf{y}_{1, \dots, j-1}] \cdot \frac{v(\mathbf{y}_{1, \dots, j-1})}{\varepsilon^{(k)}} \cdot \frac{v(\mathbf{y})}{v(\mathbf{y}_{1, \dots, j-1})} \cdot \Pr_{X_j | X^{j-1} = \mathbf{y}_{1, \dots, j-1}}[y_j] \quad (\text{Eq. (1)}) \\ &= \Pr_{X^j}[\mathbf{y}] \cdot \frac{v(\mathbf{y})}{\varepsilon^{(k)}}.\end{aligned}$$

## Ideal “attacker”, variant

### Experiment 11 ( $\hat{P}$ )

1. Let  $i^* \leftarrow [k]$ .
2. For  $j = 1$  to  $m$ :
  - 2.1 Let  $R \leftarrow \{0, 1\}^{m \times \ell}$ , conditioned on  $R_{1,\dots,j-1} = \hat{R}_{1,\dots,j-1}$ .
  - 2.2 If  $(\widetilde{P^{(k)}}, V^{(k)}(R)) = 1^k$ , set  $\hat{R}_{j,i^*} = R_{j,i^*}$ . Else, GOTO Line 2.1.
  - 2.3 Let  $R \leftarrow \{0, 1\}^{m \times \ell}$ , conditioned on  $R_{1,\dots,j-1} = \hat{R}_{1,\dots,j-1}$  and  $R_{j,i^*} = \hat{R}_{j,i^*}$ .
  - 2.4 If  $(\widetilde{P^{(k)}}, V^{(k)}(R)) = 1^k$ , set  $\hat{R}_j = R_j$ . Else, GOTO Line 2.3.

- ▶ Let  $\hat{R}$  be the final value of  $\hat{R}$  in  $\hat{P}$ .
- ▶  $\hat{R} \sim (R | (\widetilde{P^{(k)}}, V^{(k)}(R)) = 1^k)$
- ▶ Let  $\hat{N}$  be the # of Step-2.3-samples done in  $\hat{P}$ .

### Lemma 12

$$\Pr \left[ \text{win}(\hat{R}, \hat{N}) \right] \geq 1 - \frac{1}{q}$$

## From ideal to real

Let  $\hat{\mathbf{R}}_i := \hat{\mathbf{R}}|_{i^*=i}$  ( $= \hat{\mathbf{R}}$ ) and  $\tilde{\mathbf{R}}_i|_{i^*=i}$ .

### Proposition 13

$$D(\hat{\mathbf{R}}, \hat{\mathbf{N}} \| \tilde{\mathbf{R}}, \tilde{\mathbf{N}}) \leq \frac{1}{k} \sum_{i \in [k]} D(\hat{\mathbf{R}}_i \| \tilde{\mathbf{R}}_i).$$

Proof: HW.

### Lemma 14 (main lemma)

$$\sum_{i \in [k]} D(\hat{\mathbf{R}} \| \tilde{\mathbf{R}}_i) \leq D(\hat{\mathbf{R}} \| \mathbf{R})$$

- ▶ By Lecture 7 (Thm. 7),  $D(\hat{\mathbf{R}} \| \mathbf{R}) \leq \log \frac{1}{\Pr[(\hat{\mathbf{P}}^{(k)}, \mathbf{V}^{(k)}(\mathbf{R})) = 1^k]} = \log \frac{1}{\varepsilon^{(k)}}$
- ▶ Let  $\alpha := \Pr[\text{win}(\hat{\mathbf{R}}, \hat{\mathbf{N}})]$  and  $\beta := \Pr[\text{win}(\tilde{\mathbf{R}}, \tilde{\mathbf{N}})]$ .
- ▶ Lemma 14  $\implies \alpha \cdot \log \frac{\alpha}{\beta} \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)} \implies \beta \geq 2^{\log \alpha + \frac{1}{\alpha k} \log \varepsilon^{(k)}}$
- ▶ Lemma 12  $\implies \alpha \geq 1 - \frac{1}{q} \geq 2^{-\frac{2}{q}} \geq 2^{\frac{\log \varepsilon^{(k)}}{k}}$
- ▶ We conclude that  $\beta \geq 2^{\frac{4}{k} \log \varepsilon^{(k)}} = \sqrt[k/4]{\varepsilon^{(k)}}. \square$

## Proving Lemma 14

### Lemma 15

Let  $Z = \{Z_{ij}\}_{(i,j) \in [k] \times [m]}$  be iids, let  $W$  be an event, and let  $D_i(z) = \prod_{j=1}^m \Pr[Z_{j,i} = z_{i,j} | Z_{1,\dots,j-1} = z_{1,\dots,j-1}] \cdot \Pr[Z_{j,-i} = z_{i,j-1} | Z_{1,\dots,j-1} = z_{1,\dots,j-1} \wedge Z_{j,i} = z_{i,j} \wedge W]$ . Then  $\sum_{i=1}^k D(Z_W \| D_i) \leq D(Z_W \| Z)$ .

Letting  $Z = \mathbf{R}$  and  $W$  be the event  $(\widetilde{\mathbf{P}}^{(k)}, V^{(k)}(\mathbf{R})) = 1^k$ , Lemma 15 yields that  $\sum_{i \in [k]} D(\widehat{\mathbf{R}} \| \widetilde{\mathbf{R}}_i) = \sum_{i \in [k]} D(\mathbf{R}|_W \| \widetilde{\mathbf{R}}_i) \leq D(\mathbf{R}|_W \| \mathbf{R}) = D(\widehat{\mathbf{R}} \| \mathbf{R})$ .  $\square$

Proof: (of Lemma 15) We prove for  $m = k = 2$ .

- ▶ Let  $X = Z_1$  and  $Y = Z_2$
- ▶  $U(x_1, x_2, y_1, y_2) := \Pr_{(X,Y)}[(x_1, x_2, y_1, y_2)]$
- ▶  $C(x_1, x_2, y_1, y_1) := (X|_W)(x_1, x_2, y_1, y_1)$
- ▶  $Q(x_1, x_2, y_1, y_1) := \Pr[X_1 = x_1 | W] \cdot \Pr[X_2 = x_2 | W] \cdot \Pr[Y_1 = y_1 | W, X = (x_1, x_2)] \cdot \Pr[Y_2 = y_2 | W, X = (x_1, x_2)]$
- ▶ We write  $\frac{C(x_1, x_2, y_1, y_1)}{U(x_1, x_2, y_1, y_1)} = \frac{\Pr[X_1 = x_1 | W] \cdot \Pr[Y_1 = y_1 | W, X = (x_1, x_2)]}{\Pr[X_1 = x_1] \cdot \Pr[Y_1 = y_1]} \cdot \frac{\Pr[X_2 = x_2 | W] \cdot \Pr[Y_2 = y_2 | W, X = (x_1, x_2)]}{\Pr[X_2 = x_2] \cdot \Pr[Y_2 = y_2]} \cdot \frac{C(x_1, x_2, y_1, y_1)}{Q(x_1, x_2, y_1, y_1)}$

## Proving Lemma 15, cont.

$$\begin{aligned} D(C||U) &= \mathbb{E}_{(x_1, x_2, y_1, y_2) \leftarrow C} \left[ \log \frac{\Pr[X_1 = x_1|W] \cdot \Pr[Y_1 = y_1|W, X = (x_1, x_2)]}{\Pr[X_1 = x_1] \cdot \Pr[Y_1 = y_1]} \right] \\ &+ \mathbb{E}_{(x_1, x_2, y_1, y_2) \leftarrow C} \left[ \log \frac{\Pr[X_2 = x_2|W] \cdot \Pr[Y_2 = y_2|W, X = (x_1, x_2)]}{\Pr[X_2 = x_2] \cdot \Pr[Y_2 = y_2]} \right] \\ &+ \mathbb{E}_{(x_1, x_2, y_1, y_2) \leftarrow C} \left[ \log \frac{C(x_1, x_2, y_1, y_2)}{Q(x_1, x_2, y_1, y_2)} \right]. \end{aligned}$$

It follows that

$$\begin{aligned} D(C||U) &= D(X_1|W, X_2|W, X_1, Y_1|W, X, Y_2|W, X, Y_1||X_1, X_2|W, X_1, Y_1, Y_2|W, X, Y_1) \\ &+ D(X_2|W, X_1|W, X_2, Y_2|W, X, Y_1|W, X, Y_2||X_2, X_1|W, X_2, Y_2, Y_1|W, X, Y_2) \\ &+ D(C||Q), \end{aligned}$$

and the proof follows since  $D(\cdot||\cdot) \geq 0$ .  $\square$

## Parallel repetition of interactive proofs

- ▶ Similar proof to the public-coin proof we gave above.
- ▶ In each round, the attacker  $\tilde{P}$  samples **random continuations** of  $(\tilde{P}^{(k)}, V^{(k)})$ , till he gets an accepting execution.
- ▶ Why fails us to extend this approach for non-public-coin interactive arguments?

## Section 3

# **Parallel amplification for any interactive argument**

## Parallel amplification theorem for any protocol

- ▶ Can we amplify the security of any interactive argument “in parallel”?
- ▶ Yes we can!